Rancangan Kriptografi *Block Cipher* 128-*bit* Menggunakan Motif Anyaman *Rejeng* pada *Gedek*

[1]Sri Kusbiyanti, [2] Alz Danny Wowor
Fakultas Teknologi Informasi
Universitas Kristen Satya Wacana
Jl. Diponegoro 52-60, Salatiga 50771, Indonesia
Email: [1]672010149@student.uksw.edu, [2]alzdanny.wowor@staff.uksw.edu.

Abstract

Cryptography is one of the solutions that can solve data security problems. One of the cryptography used is block cipher. Many cryptographic block ciphers were made and have been solved by the cryptanalyst. The renewal of cryptography should be frequently created in order to handle cryptographic attack by cryptanalyst that more variant. In designing cryptography 128-bit block cipher is by utilizing new rejeng gedek plaited pattern as taking patterns in the plaintext and randomization pattern on the key. The results of this research show a Rejeng gedek pattern can randomization plaintext well and is a cryptographic technique because it can perform encryption and decryption process. In additional, the design is fulfill 5-tuples that can be included in a cryptographic system.

Keywords: *Block Cipher, Cryptography, Symmetric Key, Rejeng, Gedek, Correlation*

Abstrak

Kriptografi adalah salah satu penyelesaian yang dapat mengatasi masalah keamanan data. Salah satu kriptografi yang digunakan yaitu *block cipher*. Banyak kriptografi *block cipher* yang dibuat dan sudah dipecahkan oleh kriptanalis. Pembaharuan perlu sering diciptakan untuk mengatasi serangan kriptanalis agar kriptografi lebih variatif. Dalam merancang kriptografi *block cipher* 128-bit baru yaitu dengan memanfaatkan motif anyaman *rejeng gedek* sebagai pola pengambilan pada plainteks dan pola pengacakan pada kunci. Hasil dari penelitian ini menunjukan pola *rejeng gedek* dapat melakukan pengacakan plainteks dengan baik dan merupakan sebuah teknik kriptografi karena dapat melakukan proses enkripsi dan dekripsi. Selain itu perancangan ini sudah memenuhi *5-tuple* sehingga dapat dikatakan sebagai sistem kriptografi.

Kata Kunci : *Cipher Blok,* Kriptografi, Kunci Simetris, *Rejeng*, *Gedek*, Korelasi

---

[1] Mahasiswa Program Studi Teknik Informatika, Fakultas Teknologi Informasi Universitas Kristen Satya Wacana, Salatiga.
[2]Staff pengajar Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana, Salatiga.